

New Sequential Methods for Detecting Portscanners^{*}

Xinjia Chen

First submitted in April 2012

Abstract

In this paper, we propose new sequential methods for detecting port-scan attackers which routinely perform random “portscans” of IP addresses to find vulnerable servers to compromise. In addition to rigorously control the probability of falsely implicating benign remote hosts as malicious, our method performs significantly faster than other current solutions. Moreover, our method guarantees that the maximum amount of observational time is bounded. In contrast to the previous most effective method, Threshold Random Walk Algorithm, which is explicit and analytical in nature, our proposed algorithm involve parameters to be determined by numerical methods. We have developed computational techniques such as iterative mini-max optimization for quick determination of the parameters of the new detection algorithm. A framework of multi-valued decision for testing portscanners is also proposed.

1 Introduction

As Internet becomes pervasive to our society, it is increasingly important to develop high performance network intrusion detection system (NIDS) to identify an attacker to allow for protective response to mitigate or fully prevent damage. An important need in such NIDS is prompt response: the sooner a NIDS detects malice, the lower the resulting damage. At the same time, a NIDS should not falsely implicate benign remote hosts as malicious [3, 4, 6]. There are many types of network intrusions. An extremely dangerous one is the “portscans” intrusion. A port-scan is an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service [7, 9, 10].

In recent years, some detection schemes have been developed by virtue of statistical hypothesis testing. For example, the problem of detecting port-scan attacks has been addressed in the framework of testing a binomial parameter. In this direction, adaptive methods such as the Sequential Probability Ratio Tests [11] have been explored for fast detection of port-scan attacks. However, these techniques generally suffers from two drawbacks. First, the maximum number

^{*}The author had been previously working with Louisiana State University at Baton Rouge, LA 70803, USA, and is now with Department of Electrical Engineering, Southern University and A&M College, Baton Rouge, LA 70813, USA; Email: chenxinjia@gmail.com.

of required observations is not deterministically bounded. Hence, there is a probability that the detection time is extremely long. Second, the existing detection algorithms usually attempt to be optimal for only a few parametric values and consequently the average performance for other parametric values may be very poor. In order to overcome these limitations, we propose a new methods for fast detection of port-scan attacks in the general framework of multistage tests of hypotheses.

The remainder of the paper is organized as follows. In Section 2, we consider the problem of testing port-scan attack. In particular, we discuss the widely accepted binomial model and the threshold random walk detection algorithm. In Section 3, we introduce new sequential algorithm for detecting port-scan attacks. In Section 4, a framework of multi-valued decision for testing portscanners is proposed. Section 5 is the conclusion.

2 Binomial Model

A major characteristics of scanners is that they have higher chance than legitimate remote hosts to choose hosts which do not exist or do not have the requested service activated, since they lack precise knowledge of which hosts and ports on the target network are currently active [4, 6, 10]. Based on this observation, a detection problem has been formulated to provide the basis for an on-line algorithm whose goal is to reduce the number of observed connection attempts (compared to previous approaches) to flag malicious activity, while bounding the probabilities of missed detection and false detection. In this direction, a widely accepted model is the binomial model [4, 9] described in the sequel.

We shall adopt the description of [4] for the binomial model used for the detection of port-scan attacks. The activity that a remote source r makes a connection attempt to a local destination l can be considered as a random event. A frequent method to model such event is to classify the outcome of the attempt as either a “success” or a “failure”, where the latter corresponds to a connection attempt to an inactive host or to an inactive service on an otherwise active host. More formally, for a given r , let X_i be a random variable that represents the outcome of the first connection attempt by r to the i -th distinct local host, where

$$X_i = \begin{cases} 1 & \text{if the connection attempt is a success,} \\ 0 & \text{if the connection attempt is a failure} \end{cases} \quad (1)$$

As illustrated in [4, 5], it is reasonable to assume that X_i , $i = 1, 2, \dots$ are independent and identically Bernoulli random variables such that

$$\Pr\{X_i = 1\} = 1 - \Pr\{X_i = 0\} = p,$$

where $p \in (0, 1)$ is the success rate of making a connection. Usually, the success rate p is unknown and varying for different types of users. However, the success rate p of a scanner is normally very

low, while the success rate p of a benign user is high. By appropriate choosing values of threshold values p_0 and p_1 such that $0 < p_0 < p_1 < 1$ based on empirical data analysis of relevant networks, the hypothesis that “the host is a scanner” can be formulated as $\mathcal{H}_0 : p \leq p_0$. Similarly, the hypothesis that “the host is a benign user” can be formulated as $\mathcal{H}_1 : p \geq p_1$. This amounts to the problem of testing statistical hypotheses

$$\mathcal{H}_0 : p \leq p_0 \quad \text{versus} \quad \mathcal{H}_1 : p \geq p_1$$

based on X_i , $i = 1, 2, \dots$. Throughout the remainder of this paper, let $\Pr\{E \mid p\}$ denote the probability of event E associated with p . To control the probabilities of making wrong decisions, it is typically required that

$$\Pr\{\text{Reject } \mathcal{H}_0 \mid p\} \leq \alpha \text{ for all } p \in (0, p_0], \quad \Pr\{\text{Reject } \mathcal{H}_1 \mid p\} \leq \beta \text{ for all } p \in [p_1, 1) \quad (2)$$

where $\alpha, \beta \in (0, 1)$ are some pre-specified numbers. In order to minimize the potential damage of network intrusion and control the probability of false alarm, it is desirable to make this detection as quickly as possible, but with a high probability of being correct. The above formulation of the port-scanner detection problem has been proposed by a number of researchers and many detection algorithms have been developed. One of the most effective algorithms for early scan detection is the Threshold Random Walk Algorithm (TRWA) developed in [4, 5], which is represented in the following section.

3 Threshold Random Walk Algorithm

The widely cited Threshold Random Walk Algorithm [4] is derived from the famous Sequential Probability Ratio Test (SPRTs) invented by Abraham Wald [11] in the War time in response to the demand of efficient testing of ammunition power. Define relative frequency $\hat{p}_n = \frac{\sum_{i=1}^n X_i}{n}$ for $n = 1, 2, \dots$. The idea of TRWA is to continuously observe the probability ratio

$$\frac{\Pr\{X_1, \dots, X_n \mid p_0\}}{\Pr\{X_1, \dots, X_n \mid p_1\}} = \exp \left(n \left[\hat{p}_n \ln \frac{p_0}{p_1} + (1 - \hat{p}_n) \ln \frac{1 - p_0}{1 - p_1} \right] \right)$$

for $n = 1, 2, \dots$. The observational process is continued until $\frac{\Pr\{X_1, \dots, X_n \mid p_0\}}{\Pr\{X_1, \dots, X_n \mid p_1\}} \leq k_0$ or $\frac{\Pr\{X_1, \dots, X_n \mid p_0\}}{\Pr\{X_1, \dots, X_n \mid p_1\}} \geq k_1$ for some positive integer n , where $k_0 < k_1$ are two pre-specified positive integers for controlling the probability of making wrong decisions. At the termination of the observational process, a decision is made as follows:

If $\frac{\Pr\{X_1, \dots, X_n \mid p_0\}}{\Pr\{X_1, \dots, X_n \mid p_1\}} \leq k_0$, then declare the source r as a benign user. If $\frac{\Pr\{X_1, \dots, X_n \mid p_0\}}{\Pr\{X_1, \dots, X_n \mid p_1\}} \geq k_1$, then declare the source r as a scanner.

It can be shown that TRWA has the following properties: If $0 < k_0 = \alpha < 1 < \frac{1}{\beta} = k_1$, then the TRWA ensures the risk requirement (2). Moreover, the average number of observations is minimized for both p_0 and p_1 among all possible tests such that $\Pr\{\text{Reject } \mathcal{H}_0 \mid p_0\} \leq \alpha$ and $\Pr\{\text{Reject } \mathcal{H}_1 \mid p_1\} \leq \beta$.

Despite its remarkable simplicity and optimality for threshold values, the TRWA has the following major drawbacks. First, the number of observations is not bounded by a deterministic number. In the extreme case, the detection time can be unacceptably long. Second, as a consequence of the fact that TRWA is optimal when the true success rate p assumes value p_0 or p_1 , the average performance can be very poor when the true rate of success differs from p_0 and p_1 . Since the choice of threshold values p_0 and p_1 is based on empirical data analysis and is thus somewhat arbitrary, the performance of the detection algorithm is important for p taking values different from p_0 and p_1 . To overcome these drawbacks, we propose to develop a detection method in the next section.

4 New Detection Algorithm

Our new detection algorithm depends on 3 positive parameters a, b and ζ , which are to be determined by a computational method to guarantee the risk requirement. The parameter ζ is called the *risk tuning parameter*. The parameters a and b are referred to as *weighting coefficients*. Let the relative frequency \hat{p}_n be defined as before. For the ease of describing our detection algorithm, define new random variables

$$Y_n = \begin{cases} \ln \frac{1}{1-p_0} & \text{for } \hat{p}_n = 0, \\ \hat{p}_n \ln \frac{\hat{p}_n}{p_0} + (1 - \hat{p}_n) \ln \frac{1-\hat{p}_n}{1-p_0} & \text{for } 0 < \hat{p}_n < 1, \\ \ln \frac{1}{p_0} & \text{for } \hat{p}_n = 1 \end{cases}$$

$$Z_n = \begin{cases} \ln \frac{1}{1-p_1} & \text{for } \hat{p}_n = 0, \\ \hat{p}_n \ln \frac{\hat{p}_n}{p_1} + (1 - \hat{p}_n) \ln \frac{1-\hat{p}_n}{1-p_1} & \text{for } 0 < \hat{p}_n < 1, \\ \ln \frac{1}{p_1} & \text{for } \hat{p}_n = 1 \end{cases}$$

for $n = 1, 2, \dots$. We are now in a position to state the stopping and decision rules of our detection algorithm in the sequel.

4.1 Stopping and Decision Rules

Assume that the risk tuning parameter and weighting coefficients can be determined to satisfy the risk requirement (2), our detection algorithm can be described as follow.

Continue taking observations until $Y_n \geq \frac{1}{n} \ln \frac{1}{\zeta a}$, $\hat{p}_n \geq p_0$ or $Z_n \geq \frac{1}{n} \ln \frac{1}{\zeta b}$, $\hat{p}_n \leq p_1$ for some positive integer n . At the termination of observational process, make the following decision: If $Z_n \geq \frac{1}{n} \ln \frac{1}{\zeta b}$, $\hat{p}_n \leq p_1$, then declare the source r as a scanner. If $Y_n \geq \frac{1}{n} \ln \frac{1}{\zeta a}$, $\hat{p}_n \geq p_0$, then declare the source r as a benign user.

For $p_0 = 0.2$, $p_1 = 0.8$, our stopping and decision rules with $\zeta = 1$ and $a = b = 0.1$ can be shown by Figure 1. The lower shaded area represents the acceptance region of \mathcal{H}_0 . The upper shaded area represents the rejection region of \mathcal{H}_0 . The blue line with star symbols represents

a sample path. The observational process is continued until the sample path hit either the acceptance region of rejection region of \mathcal{H}_0 . If the sample path hits the acceptance region of \mathcal{H}_0 , then declare that r is a scanner. If the sample path hits the rejection region of \mathcal{H}_0 , then declare that r is a benign user.

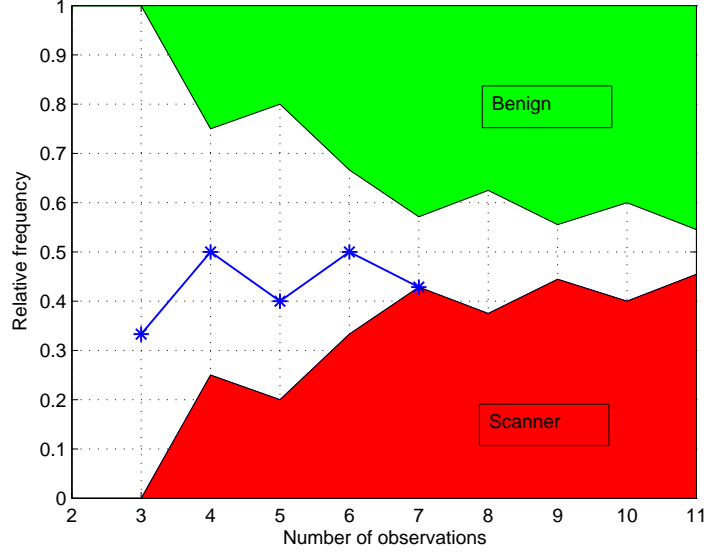


Figure 1: An illustration of new detection algorithm

4.2 Determination of Risk Tuning Parameter and Weighting Coefficients

Given that our detection algorithm can be parameterized as in Section 4.1, we need to determine the risk tuning parameter ζ and weighting coefficients a, b so that the required number of observations is as small as possible, while guaranteeing the risk requirement (2). The computational process for accomplishing this task is called *risk tuning*. Clearly, the risk requirement is satisfied if ζ is sufficiently small. This implies that if the weighting coefficients are given, one can determine the risk tuning parameter ζ to meet the risk requirement by the following two steps: First, find the maximum number, $\underline{\zeta}$, in the set $\{2^{-i} : i \in \mathbb{N}\}$, where \mathbb{N} is the set of natural numbers, such that the risk requirement is satisfied when the risk tuning parameter ζ assumes value $\underline{\zeta}$. Second, apply a bisection search method to obtain a number ζ^* as large as possible from interval $[\underline{\zeta}, 2\underline{\zeta})$ such that the risk requirement is satisfied when the risk tuning parameter ζ assumes value ζ^* . However, these two steps are not sufficient to produce a detection algorithm of satisfactory efficiency if the weighting coefficients are not properly chosen. To overcome this limitation, we observe that to make a detection algorithm efficient, it is an effective approach to make the detection algorithm efficient when the success rate p assumes values p_0 and p_1 . This is a consequence of the fact that $\Pr\{\text{Accept } \mathcal{H}_0 \mid p\}$ is non-increasing with respect to $p \in (0, 1)$. Due to the monotonicity of the operating characteristic function, it suffices to ensure $\Pr\{\text{Reject } \mathcal{H}_0 \mid p_0\} \leq \alpha$ and

$\Pr\{\text{Reject } \mathcal{H}_1 \mid p_1\} \leq \beta$ to satisfy the risk requirement (2). Define

$$A = \frac{\alpha}{\Pr\{\text{Reject } \mathcal{H}_0 \mid p_0\}}, \quad B = \frac{\beta}{\Pr\{\text{Reject } \mathcal{H}_1 \mid p_1\}}$$

$$Q = \max\{A, B\}, \quad R = \min\{A, B\}$$

as functions of a , b and ζ . For purpose of developing an efficient detection algorithm satisfying the risk requirement, we propose to determine risk tuning parameter ζ and weighting coefficients a , b such that Q is minimized under the constraint that R is no less than 1. This task can be accomplished by applying the iterative minimax optimization algorithm described as follows.

▽ Set the maximum number of iterations as k_{\max} . Choose the initial values of weighting coefficients as $a = \alpha$ and $b = \beta$. Let $\hat{Q} \leftarrow \infty$ and $k \leftarrow 0$.

▽ While $k \leq k_{\max}$, do the following:

- ◇ Use a bisection search method to determine a number $\zeta^* > 0$ as large as possible for ζ such that the value of R associated with a , b and ζ^* is no less than 1. Let A^* , B^* and Q^* respectively denote the corresponding values of A , B and Q .
- ◇ If $Q^* < \hat{Q}$, then let $\hat{a} \leftarrow \zeta^* a$, $\hat{b} \leftarrow \zeta^* b$ and $\hat{Q} \leftarrow Q^*$. If $A^* = Q^*$, then let $a \leftarrow \zeta^* a(1 + \frac{Q^*-1}{5})$. If $B^* = Q^*$, then let $b \leftarrow \zeta^* b(1 + \frac{Q^*-1}{5})$. Let $k \leftarrow k + 1$.

▽ Return $\zeta = 1$ as the desired risk tuning parameter and \hat{a}, \hat{b} as the weighting coefficients.

The intuition behind this algorithm is that $\Pr\{\text{Reject } \mathcal{H}_0 \mid p_0\}$ and $\Pr\{\text{Reject } \mathcal{H}_1 \mid p_1\}$ are “roughly” increasing with respect to a and b , respectively, when the risk tuning parameter ζ is fixed.

In the execution of the algorithm, we need to compute the probabilistic terms like $\Pr\{\text{Reject } \mathcal{H}_0 \mid p_0\}$ and $\Pr\{\text{Reject } \mathcal{H}_1 \mid p_1\}$. These quantities can be computed by the path counting method of [2] or the recursive algorithm of [8].

4.3 Maximum Number of Observations

One salient feature of the above algorithm is that the maximum number of observations is absolutely bounded. Moreover, the maximum number is the least integer no less than m which satisfies the following equations:

$$\left(\frac{1-p_0}{1-z}\right)^{1-z} \left(\frac{p_0}{z}\right)^z = (\zeta a)^{\frac{1}{m}},$$

$$\left(\frac{1-p_1}{1-z}\right)^{1-z} \left(\frac{p_1}{z}\right)^z = (\zeta b)^{\frac{1}{m}},$$

where $z \in (p_0, p_1)$. To solve the above equations for m , we first eliminate m and obtain

$$\frac{\ln \left[\left(\frac{1-p_0}{1-z} \right)^{1-z} \left(\frac{p_0}{z} \right)^z \right]}{\ln \left[\left(\frac{1-p_1}{1-z} \right)^{1-z} \left(\frac{p_1}{z} \right)^z \right]} = \frac{\ln(\zeta a)}{\ln(\zeta b)},$$

from which we find the root $z = z^*$ by a bisection search method. Afterward, we substitute $z = z^*$ into the first equation to obtain the corresponding $m = m^*$. Then, the maximum number of observations is equal to $\lfloor m^* \rfloor + 1$. It should be noted that, in the special case of $a = b$, we have

$$(1-z) \ln \frac{1-p_0}{1-p_1} + z \ln \frac{p_0}{p_1} = 0,$$

from which we obtain

$$z^* = \frac{\ln \frac{1-p_0}{1-p_1}}{\ln \frac{(1-p_0)p_1}{(1-p_1)p_0}}$$

and a closed-formed formula for m^* .

4.4 Comparison with TRWA

We have conducted numerical experiments for comparing our detection scheme with TRWA. For the case of $p_0 = 0.1$, $p_1 = 0.15$ and $\alpha = \beta = 0.1$, the risks of our detection scheme (with $\zeta = 0.96$, $a = b = 0.1$) and TRWA are respectively shown by the blue and green plots in Figure 2. With the same configuration, the ratio between the average number of observations of our detection algorithm to that of TRWA is shown in Figure 3. Our computation shows that the new detection algorithm requires a much smaller number of connection attempts to detect a scanner as compared to TRWA.

5 Multi-Valued Decision

As can be seen from the risk requirement (2), there is no specification imposed for users with success rate $p \in (p_0, p_1)$. This implies that those users can be arbitrarily classified as either scanners or benign users. In applications, p_0 is usually chosen as a number close to 0, while p_1 is chosen as a number close to 1. Therefore, there exists a wide gap between p_0 and p_1 . This indicates that there is a large portion of “marginal” users being cast into either the category of scanners or benign users. In view of this situation, we propose to classify the users as three categories: scanner, marginal, and benign. Specifically, let p_0 and p_1 be two threshold values such that $0 < p_0 < p_1 < 1$. We propose to test the following three hypotheses:

$$\mathcal{H}_0 : p \leq p_0, \quad \mathcal{H}_1 : p_0 < p < p_1, \quad \mathcal{H}_2 : p \geq p_1$$

where hypotheses \mathcal{H}_0 , \mathcal{H}_1 and \mathcal{H}_2 corresponds to the categories of “scanner”, “marginal”, and “benign”. Based on the classification, different actions are taken for the corresponding categories.

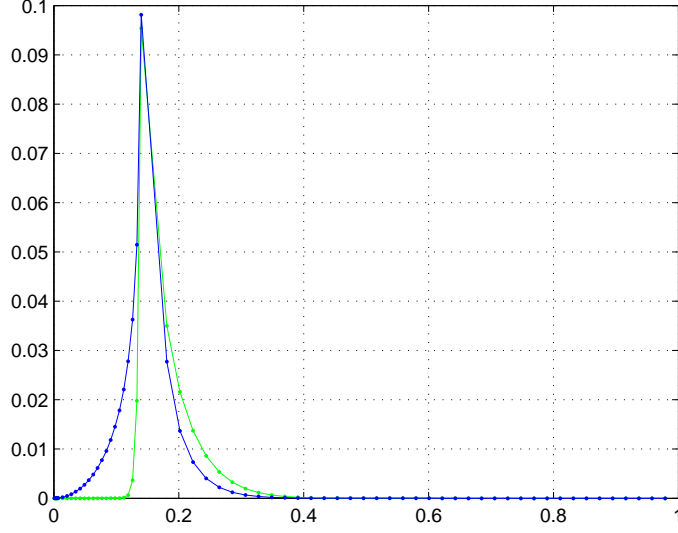


Figure 2: Comparison of risks

To control the probabilities of making wrong decisions, we impose the following requirement:

$$\begin{aligned} \Pr\{\text{Reject } \mathcal{H}_0 \mid p\} &\leq \delta_0 \quad \text{for } p \in (0, p'_0], \\ \Pr\{\text{Reject } \mathcal{H}_1 \mid p\} &\leq \delta_1 \quad \text{for } p \in [p''_0, p'_1], \\ \Pr\{\text{Reject } \mathcal{H}_2 \mid p\} &\leq \delta_2 \quad \text{for } p \in [p''_1, 1) \end{aligned}$$

where $0 < p'_0 < p_0 < p''_0 < p'_1 < p_1 < p''_1 < 1$ and $\delta_i \in (0, 1)$ for $i = 1, 2, 3$. The intervals (p'_0, p''_0) and (p'_1, p''_1) are called indifference zones, since no specification is imposed for controlling the probability of making wrong decisions for p contained in these intervals. This problem is actually a special case of the general problem of testing multiple hypotheses, which has been systematically addressed in our recent paper [1]. The techniques in [1] offer a complete solution to the present problem of testing triple hypotheses on the success rate p . As an illustration, assume that

$$\begin{aligned} \delta_0 &= \delta_1 = \delta_2 = 0.1, \\ p_0 &= \frac{1}{3}, \quad p_1 = \frac{2}{3}, \end{aligned}$$

and

$$p'_0 = p_0 - \frac{1}{9}, \quad p''_0 = p_0 + \frac{1}{9}, \quad p'_1 = p_1 - \frac{1}{9}, \quad p''_1 = p_1 + \frac{1}{9}.$$

By virtue of the technique of [1], we have obtained a sequential testing scheme shown by Figure 4, where the bottom, middle and upper shaded areas represent the acceptance regions of \mathcal{H}_0 , \mathcal{H}_1 and \mathcal{H}_2 , respectively. The stopping and decision rules can be stated as follows:

If the sample path, which can be represented by the plot of the relative frequency \hat{p}_n versus the number n of observations, hits a shaded region, then terminate the observational process. At

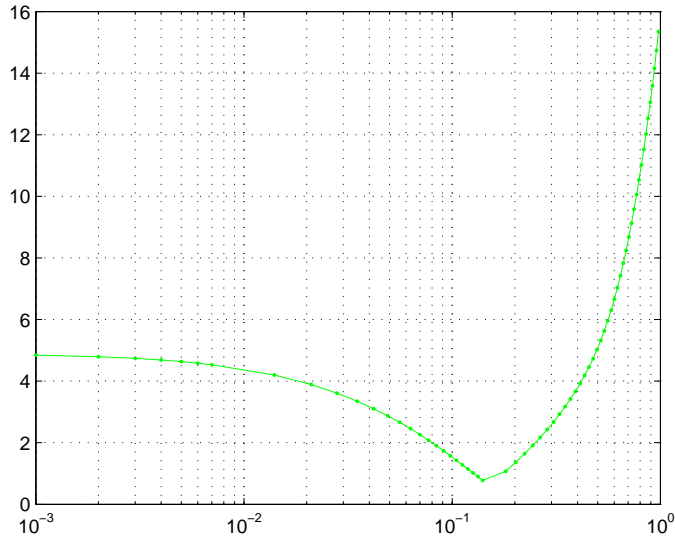


Figure 3: Comparison of average number of observations

the termination of the observational process, accept the hypothesis of which the acceptance region is hit by the sample path.

In Figure 5, we plot the risk, $\Pr\{\text{The decision is incorrect} \mid p\}$, versus the success rate p . It can be seen that the risk requirement is satisfied for any $p \in (0, 1)$ not contained in the indifference zones.

6 Conclusion

We have developed new sequential methods for detecting portscanners. In addition to guaranteeing the risk requirement, our algorithm is efficient when the success rate assumes values other than the threshold values. Moreover, the required number of observations is absolutely bounded. Furthermore, we have proposed a framework of multi-valued decision for testing portscanners.

References

- [1] X. Chen, “A new framework of multistage hypothesis tests,” arXiv.0809.3170[math.ST], multiple versions, first submitted in September 2008.
- [2] S. Franzén S., “Fixed length sequential confidence intervals for the probability of response,” *Sequential Analysis*, 20, 45–54, 2001.

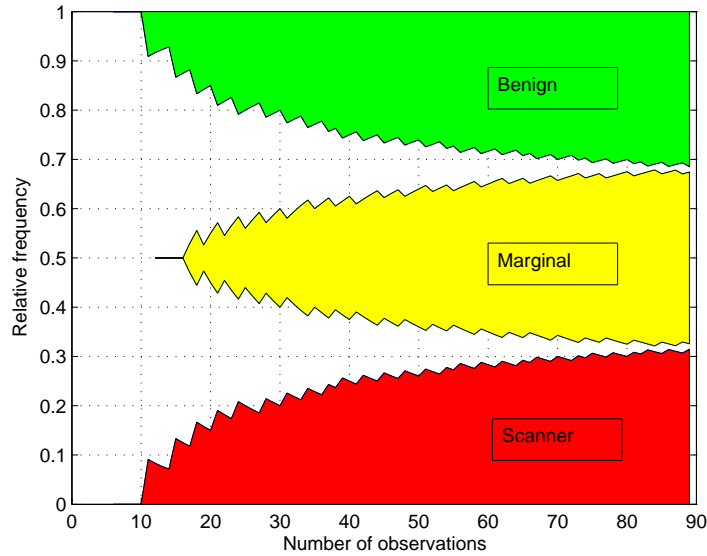


Figure 4: Triple Hypothesis Testing

- [3] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, and D. Wolber, “A network security monitor,” *Proc. IEEE Symposium on Research in Security and Privacy*, pp. 296–304, 1990.
- [4] J. Jung, V. Paxson, A. Berger, and H. Balakrishnan, “Fast portscan detection using sequential hypothesis testing,” *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 2004.
- [5] J. Jung, S. E. Schecher, and A. Berger, “Fast detection of scanning worm infections,” *Recent Advances in Intrusion Detection*, 2004, Springer.
- [6] C. Leckie and R. Kotagiri, “A probabilistic approach to detecting network scans,” *Proceedings of the Eighth IEEE Network Operations and Management Symposium*, pp. 359–372, Florence, Italy, April 2002.
- [7] M. Roesch, “Snort: Lightweight intrusion detection for networks,” *Proceedings of the 13th Conference on Systems Administration*, pp. 229–238, Berkeley, CA, November 1999.
- [8] J. R. Schultz, F. R. Nichol, G. L. Elfring, and S. D. Weed, “Multiple-stage procedures for drug screening,” *Biometrics*, 29, 293–300, 1973.
- [9] S. Staniford, J. A. Hoagland, and J. M. McAlerney, “Practical automated detection of stealthy portscans,” *Proceedings of the 7th ACM Conference on Computer and Communications Security*, Athens, Greece, 2000.

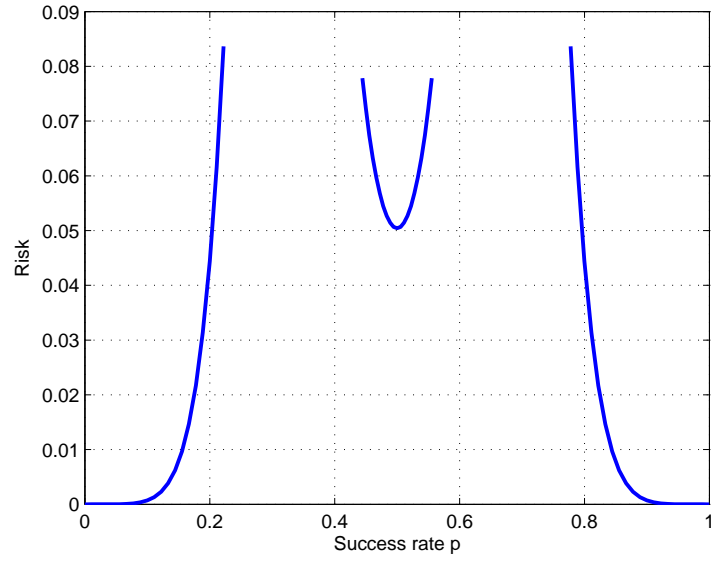


Figure 5: Risk

- [10] V. Yegneswaran, P. Barford, and J. Ullrich, “Internet intrusions: global characteristics and prevalence,” *Proceedings of the 2003 ACM SIGMETRICS*, volume 31, pp. 138–147, New York, June 2003.
- [11] A. Wald, *Sequential Analysis*, Wiley, 1947.